United States Department of Agriculture
Grain Inspection, Packers and Stockyards Administration

Program Notice **GIPSA PN-04-09** **09/23/04**

GIPSA INFORMATION TECHNOLOGY (IT) SYSTEM AUDITS

1. PURPOSE

This program notice establishes the policy and procedures for auditing IT systems in Grain Inspection, Packers and Stockyards Administration (GIPSA).

2. EFFECTIVE DATE

This action is effective upon receipt.

3. BACKGROUND

Audit trails maintain a record of system activity by system or application processes and by user activity. This policy is meant to provide general guidance in collecting and reviewing this data. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

4. POLICY

Audit trails in GIPSA will be used for the following:

- **Individual Accountability.** The audit trail supports accountability by providing a trace of user actions. Audit trail analysis will be used to ensure users are using GIPSA resources for authorized purposes only.

- **Reconstruction of Events.** Audit trails will be used to support after the fact investigations of how, when, and why normal operations ceased.

- **Intrusion Detection.** Audit trails will be used to assist in intrusion detection. Intrusions can be detected in real time by examining audit records as they are created or, after the fact by examining audit records in a batch process.

- **Problem Identification.** Audit trails may also be used as online tools to help identify problems as they occur. This is often referred to as real time auditing or monitoring.

5. PROCEDURES

An audit trail will include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail should be done carefully to balance security needs with possible performance, privacy, or other costs. In general, an event record should specify:

- **Type of Event and Result.** The type of event and its result, such as failed user authentication attempts, changes to users' security information, and organization and application specific security relevant events.

- **When the Event Occurred.** The time and day the event occurred.

- **User ID Associated With the Event.**

- **Program or Command Used to Initiate the Event.**

GIPSA IT Staff will protect the audit trail information from unauthorized access. The following precautions will be taken:

- **Control Online Audit Logs.** Access to online audit logs will be strictly controlled. Only the GIPSA IT staff will have access to audit logs.

- **Separation of Duties.** GIPSA's system administrators will generate the audit logs and GIPSA's IT Operations Branch will review the logs daily. System administrators will train the IT Operations Branch in identifying unusual activity and identifying anomalies.

- **Protect Confidentiality.** The confidentiality of audit trail information will be protected. GIPSA's IT Operations Branch will secure all hard copy audit logs in a locked file cabinet. Only the GIPSA IT staff will have access to this filing. Electronic audit files will be placed on a secure networked drive with authorized access given only to those with a need to know. All audits logs over one year old will be destroyed.

6. RESPONSIBLITIES

Audit trail reports will be reviewed monthly by GIPSA's Information Systems Security Program Manager (ISSPM). The following will be considered when reviewing audit trails:

- **Follow-up Reviews.** The appropriate system level or application level administrator will review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

- **Develop Review Guidelines.** System administrators can determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.

7. QUESTIONS

Direct questions to the Information Systems Security Program Manager at (202) 720-1741.

/s/

Donna Reifschneider
Administrator